Federal Identity Credentialing

FICC Goals

- Simplify and Unify Identity Authentication for Federal Employees
- Create requirements for Physical Credentials, electronic credentials, and issuance.
- Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture

Objectives

- Compatibility between physical/logical credentials issued by multiple organizations;
- Streamlined and automated building access, visit requests, and authorization across the government;
  - Less manpower intensive building access procedures;
  - Immediate identification and subsequent denial of access for those with revoked credentials;
- Improved access to interagency electronic processes, Cross-organizational recognition and authentication of e-mail correspondents, digital signatures, and message integrity.

Charter

The Federal Identity and Credentialing Committee will make recommendations regarding establishment, demonstration, and operation of a Federal Identity Management component; and provide a focal point for the implementation of the component including support of migration to a shared service concept endorsed as part of the Federal Enterprise Architecture.

Responsibilities

- Develop Federal Government Identity Management requirements in coordination with the Architecture and Infrastructure Subcommittee of the CIO Council;
- Recommend policies, procedures and standards development to support a Federal Identity Management component;
- Oversee Federal Identity Management activities in Federal implementations;
- Provide recommendations to OMB and OPM on the establishment of identity proofing minimum requirements;
- Specify technologies needed for Federal Identity credentials in accordance with NIST guidance and standards; and
- Establish interoperability and security requirements of products and protocols related to Federal Identity Management.

Task #1

- A common policy for physical/logical credentialing for Federal Employees
- A set of minimum requirements for Identity Assurance for Federal Employees
- A common policy for PKI deployment to Federal Employees
- A consolidated acquisition for implementation
  - Consolidated SmartCard Acquisition
  - PKI Managed Service Providers

Milestones

- Release Common Policy Framework — Sep 1, 2003
- Aggregated Buy of *Credentials* — Oct 1, 2003
- Deliver Authentication Component — Oct 1, 2003
- Shared Service Migration — Dec 1, 2003

Requirements: Common Policy Framework

- Federal Identity Credentialing Guidance
  - "How to" guide for Federal entities
- Common PKI Certificate Policy
  - Consistent with FBCA Certificate Policy requirements
- Common SmartCard Policy
  - Common requirements
  - Minimum specifications
  - Minimum common data sets
- Guidance for establishing employee identity
  - Leverage existing Executive Order/Statute

Requirements: Aggregated Buy

- Consolidate requirements based on BDR responses
- Finalize aggregated buy plan
- Conduct procurement

Requirements: Shared Service Migration

- Develop criteria for PKI shared service providers
- Release acquisition strategy
- Establish PKI Shared Service Review Board
- Establish scoring matrix
- Analyze proposals
- Announce selection of PKI shared service providers
- Provide instruction on selecting a service

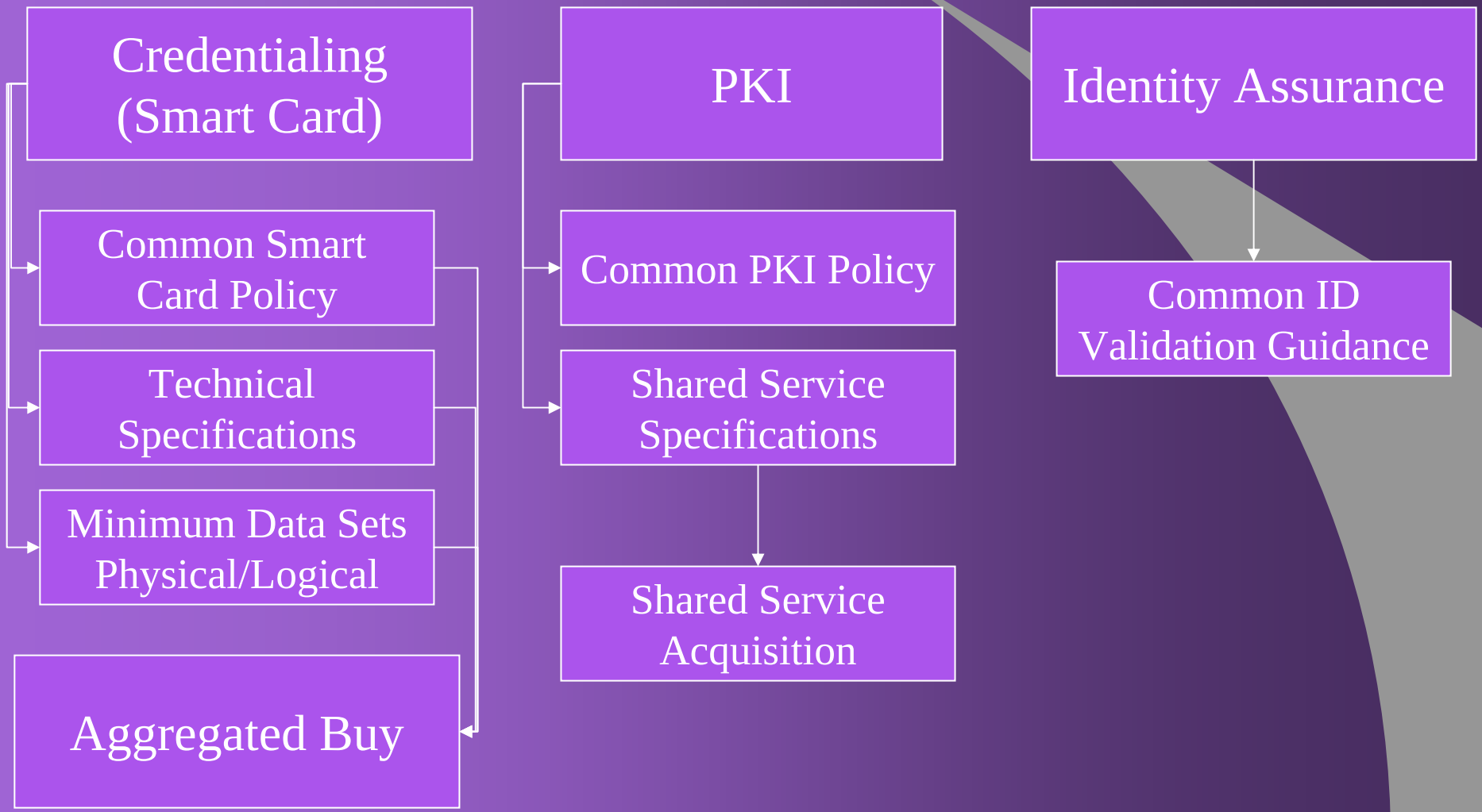
Requirements: Authentication Component

- Bundle Guidance and Policy Documents into a coherent unit.
- Develop Transition Plan for Federal agencies

Next Steps/Planning

- Task group determination:
  - What needs to be done?
  - What skill sets should be included?
- Policy Development/Review
  - Common PKI Policy
  - Common Smart Card Policy
  - Common ID Verification Requirements
- Technical Specification Development/Review
  - Physical credentials
  - Logical credentials
  - PKI
  - Identity verification

Work Teams


Credentialing (Smart Card)
Common Smart Card Policy
Technical Specifications
Minimum Data Sets Physical/Logical
Aggregated Buy
PKI
Common PKI Policy
Shared Service Specifications
Shared Service Acquisition
Identity Assurance
Common ID Validation Guidance